REMARKS

The present amendment makes editorial changes to the specification, drawings, claims and Abstract in order to conform the United States Patent Practice. Additionally, the Applicants include herewith a copy of the new Abstract on a separate page. None of the changes in the claims is intended as a surrender of any of the subject matter within the scope of the original claim language since, as noted above, all of these changes have been made solely to bring the claims into conformity with the requirements of 35 U.S.C. §112, second paragraph.

Early consideration of the application is respectfully requested.

Respectfully submitted,

_______________(Reg.No. 45,877)

Mark Bergner
SCHIFF HARDIN & WAITE
PATENT DEPARTMENT
6600 Sears Tower
Chicago, Illinois 60606-6473
(312) 258-5779
ATTORNEY FOR APPLICANT

line 19, after "devices" insert --)--;

line 20, delete ",";

line 22, replace ", that is to say" with --(i.e.,--;

line 23, replace "," with --)--;

line 24, replace ", that is to say" with --(i.e.,--;

line 25, replace ":" with --) according to the relationship:--;

line 26, replace "D (E (Z (A), sAD), pAD) = Z (A)" with -- D (E (Z (A)), sAD), pAD) = Z (A).--;

line 29, replace "A" with --Hence,--; and

line 31, replace "can thus" with --, thus, can--.

On page 5:

line 2, delete ",";

line 7, delete ","; and

after line 8, insert the following paragraph:

--While this invention has been described in connection with what are presently considered to be the most practical and preferred embodiments, it is to be understood that the invention is not limited to the disclosed embodiments, but, on the contrary, is intended to cover various modifications and equivalent arrangements included within the spirit and scope of the appended claims.--

IN THE CLAIMS:

On page 6, replace "Patent Claims" with --What is claimed is:--.

Cancel claims 1-3 without prejudice or disclaimer.

Please add new claims 4-7 as follows.

4. A method for authenticating key devices using an asymmetric encryption method in which each key device is assigned a device-specific certificate, the method comprising the steps of:

assigning each key device a group-specific ~~signature~~ public key; and

assigning each key device a group-specific signature of the device-specific certificate;

wherein a group is comprised of a limited total number of key devices.

5. The method according to claim 4, wherein the group-specific signature key and the group-specific signature of the device-specific certificate are allocated to each key device during a first initialization.

6. The method according to claim 4, wherein the steps of assigning the group-specific signature key and the group-specific signature of the device-specific certificate to an associated specific group are each determined by comparing each key device with a stored list of approved key devices.

7. The method according to claim 4, further comprising the steps of:

establishing a link between at least two key devices;

transmitting a corresponding device-specific certificate and a corresponding device-specific ~~signature~~ public key from one of the key devices to another one of the key devices, the another one of the key devices verifying authenticity of the corresponding device-specific certificate using the corresponding device-specific ~~signature~~ public key according to the relationship:

$$D(S(Z(A)), pAD) = D(E(Z(A)), sAD), pAD) = Z(A)$$

where D represents a decryption function, S(Z(A)) represents signature of the corresponding device-specific certificate, E(Z(A)) represents an encryption function of the corresponding device-specific certificate, pAD represents a signature key of an administrator, sAD represents a secret key of the administrator, and Z(A) represents the corresponding device-specific certificate.

IN THE ABSTRACT:

Delete original page 7 and replace the Abstract with Replacement Page 7, which is provided on a separate sheet attached to the amendment.

ABSTRACT

A method for authentication of key devices using an asymmetric encryption method, in which the key device is assigned a device-specific certificate. According to the invention, each key device is assigned a group-specific signature key and a group-specific signature of the certificate, with a group being composed of a limited total number of key devices.